Outline for next 2 lectures.

1. Cryptography $\Rightarrow$ relation to Bijective functions
2. Public Key Cryptography
3. RSA system
   3.1 Efficiency: Repeated Squaring.
   3.2 Correctness: Fermat’s Little Theorem.
   3.3 Construction.
Cryptography ...

What is the relation between $D$ and $E$ (for the same secret $s$)?

$m = D(E(m, s), s)$

Secret $s$

Alice $\leftrightarrow E(m, s)$ Eve $E(m, s)$ Bob

Message $m$
Excursion: Bijects.

\[ f : S \rightarrow T \] is **one-to-one mapping**.

One-to-one: \( f(x) \neq f(x') \) for \( x, x' \in S \) and \( x \neq x' \). Not 2 to 1!

\( f(\cdot) \) is **onto**

if for every \( y \in T \) there is \( x \in S \) where \( y = f(x) \).

Bijection is one-to-one and onto function.

Two sets have the same size

if and only if there is a bijection between them!

**Same size?**

\( \{ \text{red, yellow, blue} \} \) and \( \{1, 2, 3\} \)?

\[ f(\text{red}) = 1, \ f(\text{yellow}) = 2, \ f(\text{blue}) = 3. \]

\( \{ \text{red, yellow, blue} \} \) and \( \{1, 2\} \)?

\[ f(\text{red}) = 1, \ f(\text{yellow}) = 2, \ f(\text{blue}) = 2. \]

**two to one!** not one to one.

\( \{ \text{red, yellow} \} \) and \( \{1, 2, 3\} \)?

\[ f(\text{red}) = 1, \ f(\text{yellow}) = 2. \]

**Misses 3.** not onto.
Modular arithmetic examples.

\( f : S \to T \) is **one-to-one mapping**.

- one-to-one: \( f(x) \neq f(x') \) for \( x, x' \in S \) and \( x \neq y \).

\( f(\cdot) \) is **onto**

- if for every \( y \in T \) there is \( x \in S \) where \( y = f(x) \).

Recall: \( f(red) = 1, f(yellow) = 2, f(blue) = 3 \)

One-to-one if inverse: \( g(1) = red, g(2) = yellow, g(3) = blue \).

Is \( f(x) = x + 1 \pmod{m} \) one-to-one? \( g(x) = x - 1 \pmod{m} \).

Onto: range is subset of domain.

Is \( f(x) = ax \pmod{m} \) one-to-one?

- If \( \gcd(a, m) = 1, ax \neq ax' \pmod{m} \).

Injective? Surjective?

- We tend to use one-to-one and onto.

**Bijection** is one-to-one and onto function.

- Two sets have the same size
  - if and only if there is a bijection between them!
Claim: \( a^{-1} \pmod{m} \) exists when \( \gcd(a, m) = 1 \).

Fact: \( ax \neq ay \pmod{m} \) for \( x \neq y \in \{0, \ldots, m-1\} \)

Consider \( T = \{0a \pmod{m}, 1a \pmod{m}, \ldots, (m-1)a \pmod{m}\} \)

Consider \( S = \{0, 1, \ldots, (m-1)\} \)

\( S = T \). Why?

- \( T \subseteq S \) since \( ax \pmod{m} \in \{0, \ldots, m-1\} \)
- One-to-one mapping from \( S \) to \( T \)!

\[ \Rightarrow |T| \geq |S| \]

Same set.

Why does \( a \) have inverse? \( T \) is \( S \) and therefore contains 1!

What does this mean? There is an \( x \) where \( ax = 1 \).

There is an inverse of \( a \)!
Back to Cryptography ...

What is the relation between $D$ and $E$ (for the same secret $s$)?
$D$ is the inverse function of $E$!

Example:
One-time Pad: secret $s$ is string of length $|m|$.
$E(m, s)$ – bitwise $m \oplus s$.
$D(x, s)$ – bitwise $x \oplus s$.

Works because $m \oplus s \oplus s = m$
...and totally secure!
...given $E(m, s)$ any message $m$ is equally likely.

Disadvantages:
Shared secret!

Uses up one time pad..or less and less secure.
Public key cryptography.

\[ m = D(E(m, K), k) \]

Everyone knows key \( K \)!
Bob (and Eve and me and you and you ...) can encode. Only Alice knows the secret key \( k \) for public key \( K \).
(Only?) Alice can decode with \( k \).
Is public key crypto unbreakable?

We don’t really know.
...but we do it every day!!!

RSA (Rivest, Shamir, and Adleman)
Pick two large primes \( p \) and \( q \). Let \( N = pq \).
Choose \( e \) relatively prime to \((p - 1)(q - 1)\).\(^1\)
Compute \( d = e^{-1} \mod (p - 1)(q - 1) \). \( d \) is the private key!
Announce \( N(=p \cdot q) \) and \( e \): \( K = (N, e) \) is my public key!

Encoding: \( \mod (x^e, N) \).

Decoding: \( \mod (y^d, N) \).

Does \( D(E(m)) = m^{ed} = m \mod N \)?
Yes!

\(^1\)Typically small, say \( e = 3 \).
Example: \( p = 7, \ q = 11. \)

\( N = 77. \)

\((p - 1)(q - 1) = 60\)

Choose \( e = 7, \) since \( \gcd(7, 60) = 1. \)

How to compute \( d? \) \( \text{egcd}(7, 60). \)

\( 7(-17) + 60(2) = 1 \)

Confirm: \(-119 + 120 = 1\)

\( d = e^{-1} = -17 = 43 = \ (\text{mod} \ 60)\)
Important Considerations

Q1: Why does RSA work correctly? Fermat’s Little Theorem!

Q2: Can RSA be implemented efficiently? Yes, repeated squaring!
RSA on an Example.

Public Key: (77, 7)
Message Choices: {0, ..., 76}.

Message: 2

\[ E(2) = 2^e = 2^7 \equiv 128 \pmod{77} = 51 \pmod{77} \]
\[ D(51) = 51^{43} \pmod{77} \]

uh oh!

Obvious way: 43 multiplications. Ouch.

In general, \( O(N) \) multiplications in the \textit{value} of the exponent \( N \)!
That’s not great.
Repeated Squaring to the rescue.

$$51^{43} = 51^{32+8+2+1} = 51^{32} \cdot 51^{8} \cdot 51^{2} \cdot 51^{1} \pmod{77}.$$ 4 multiplications sort of...

Need to compute $51^{32} \ldots 51^{1}$?

$51^{1} \equiv 51 \pmod{77}$

$51^{2} = (51) \cdot (51) = 2601 \equiv 60 \pmod{77}$

$51^{4} = (51^{2}) \cdot (51^{2}) = 60 \cdot 60 = 3600 \equiv 58 \pmod{77}$

$51^{8} = (51^{4}) \cdot (51^{4}) = 58 \cdot 58 = 3364 \equiv 53 \pmod{77}$

$51^{16} = (51^{8}) \cdot (51^{8}) = 53 \cdot 53 = 2809 \equiv 37 \pmod{77}$

$51^{32} = (51^{16}) \cdot (51^{16}) = 37 \cdot 37 = 1369 \equiv 60 \pmod{77}$

5 more multiplications.

$$51^{32} \cdot 51^{8} \cdot 51^{2} \cdot 51^{1} = (60) \cdot (53) \cdot (60) \cdot (51) \equiv 2 \pmod{77}.$$ 

Decoding got the message back!

Repeated Squaring took 9 multiplications versus 43.
Repeated Squaring: $x^y$

Repeated squaring $O(\log y)$ multiplications versus $y$!!!

1. $x^y$: Compute $x^1, x^2, x^4, \ldots, x^{2^{\lfloor \log y \rfloor}}$.

2. Multiply together $x^i$ where the $(\log(i))$th bit of $y$ is 1.
Fermat’s Little Theorem: For prime $p$, and $a \not\equiv 0 \pmod{p}$,

$$a^{p-1} \equiv 1 \pmod{p}.$$ 

**Proof:** Consider $S = \{a \cdot 1, \ldots, a \cdot (p-1)\}$.

All different modulo $p$ since $a$ has an inverse modulo $p$. That is, $S$ contains representative of each of $1, \ldots, p-1$ modulo $p$.

$$(a \cdot 1) \cdot (a \cdot 2) \cdots (a \cdot (p-1)) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

Since multiplication is commutative.

$$a^{(p-1)}(1 \cdots (p-1)) \equiv (1 \cdots (p-1)) \pmod{p}.$$  

Each of $2, \ldots (p-1)$ has an inverse modulo $p$, solve to get...

$$a^{(p-1)} \equiv 1 \pmod{p}.$$